Kurt Salmon

Plan de continuité d'activité

Gérer efficacement les situations de crise dans le secteur de l'assurance

Juin 2012

« Il n'y a que deux types d'entreprises : celles qui sont en situation de crise et celles qui le seront »

ACA
ASSOCIATION DES COMPAGNIES D'ASSURANCES DU GRAND-DUCHÉ DE LUXEMBOURG

ALAC
Association Luxembourgeoise des Actuaires

Sommaire

Introduction aux risques de rupture d’activité

Résilience métier et plan de continuité de l’activité (PCA)

Elaborer et piloter un plan de continuité et de reprise de l’activité

Conclusions

Depuis plusieurs années, de nombreux évènements exceptionnels ont montré la vulnérabilité des pays et de leurs entreprises face à des catastrophes ou sinistres de grande ampleur

Catastrophes naturelles

Crues de la Somme (France) - 2001
Tsunami (Océan Indien) - 2004
Ouragan Katrina (Etats-Unis) - 2005

Accidents / Terrorisme

Incendie du siège du Crédit Lyonnais - 1996
Cyber attaque Sony (PSN) - 2011
Fukushima (Japon) - 2011

Défaillances d'infrastructures

Panne du système d'information d'Euronext - 2004
Arrêt des réseaux électriques nationaux (Etats-Unis) – 2008
Panne réseau RIM (Blackberry) - 2011

Risques sanitaires

Épidémie de SRAS (Hong Kong) 2003
Grippe aviaire Virus A (H5N1) en Asie et Afrique 2006

Attentats de New-York du 11 septembre 2001

- 60 milliards € de dommages directs
- 11 milliards € de pertes d'activités sur 2001 et 2002
- 108 000 emplois supprimés (Etat de New-York)

Explosion Usine AZF du **21 septembre 2001**

- 2,5 milliards € de dommages directs
- 1300 entreprises sinistrées
- 1200 emplois supprimés (Toulouse et agglomération)

Le développement des réseaux et la mondialisation des activités font prendre conscience aux entreprises de la vulnérabilité de leurs activités

Risques naturels	**Risques humains ou sanitaires**	**Risques de défaillances d'infrastructure**	**Risques partenaires**
Tremblement de terre Inondations Incendie	Erreurs Pandémie/Intoxication Malveillance	Outil de production Electricité, gaz, etc. Système d'information	Arrêt d'activité Grèves Prestataires

« Le mieux c'est que ça n'arrive pas ! »
« Plus de téléphone ? Utilisez vos portables ! »
« Comment on va faire pour prendre les commandes ? »
« Où est-ce qu'on va travailler ? »
« Disposer de solutions de repli pour le personnel et le SI »

Situation de crise

« Survenance d'un évènement exceptionnel qui vient perturber de manière significative le fonctionnement habituel »

La survenue d'incidents majeurs, même si leur probabilité d'occurrence est faible, est susceptible d'altérer de manière durable l'activité courante d'une entreprise et engendrer de multiples impacts :

Commerciaux	✓ Perte de clients ✓ Litiges commerciaux ✓ Pertes de parts de marché
Financiers	✓ Perte de trésorerie ✓ Pénalités de retard ✓ Couts majorés de reprise de l'activité
Juridiques	✓ Non respect d'obligations légales ou réglementaires ✓ Sanctions disciplinaires (et financières) ✓ Sanctions pénales
Organisation, Processus et Données	✓ Rupture de la logique des processus internes ✓ Perte d'information, génération d'erreurs ✓ Surcharge de travail, Conflit social ✓ Chômage technique
Réputation & Image de l'entreprise	✓ Perte de confiance des clients ou partenaires ✓ Perte de confiance des investisseurs, baisse significative du cours de l'action

La mise en place d'une stratégie de résilience métier doit permettre à l'entreprise d'adresser les enjeux suivants

Garantir la survie de l'entreprise	**Conquérir de nouveaux marché et rassurer les clients**	**Répondre à ses obligations légales**	**Réduire leurs primes d'assurance**

Sociétés d'assurance: comment font-elles face à un incident majeur provoquant une rupture de leur activité?

- Face à un sinistre ***exceptionnel les mesures préventives ne sont pas suffisantes***
- La « gestion de la continuité d'activité » est une approche globale (en termes d'organisation, de ressources humaines, d'outils et de systèmes) qui permet de mettre en œuvre des ***solutions de continuité en cas de survenance d'un sinistre exceptionnel.***

La continuité des activités dans la Presse

Every five years, 20% of companies will suffer a major disruption through fire, flood or storm, power failures, terrorism, or hardware/software failures. Of those companies which do not have a Business Continuity Plan, 80% fail within 13 months of such an incident. Those who successfully restore their business have seen the company value rise.

Source: Business Continuity Institute

90% of businesses that lose data from a disaster are forced to shut down within 2 years of the disaster
43% of companies who have a business continuity plan do not test it annually to ensure it works

London Chamber of Commerce

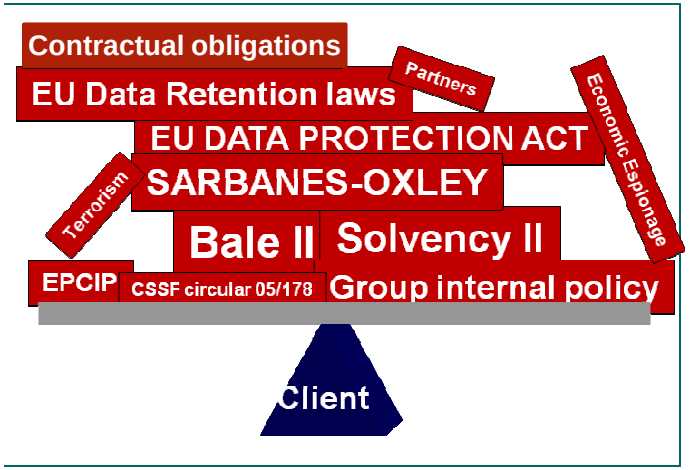
- Le degré de mise en œuvre et de déploiement d'une stratégie de continuité des activité diffère fortement entre les assureurs* :
  - ***40 % des entreprises*** *n'ont pas mis en place de programme de continuité des activités,* notamment dans les entreprises les plus petites
  - *La* ***formalisation d'outils de gestion des risques ou de bases incidents****, pouvant servir de base à la mise en place d'un plan de gestion des risques de continuité* ***est très peu développée*** *(moins de 15% des sociétés interrogées)*
  - *La fonction métier de gestion-indemnisation montre de fortes carences en termes de contrôle (internes liés aux risques opérationnels)*
  - *Un point d'attention est à porter aux activités déléguées (****BPO****) qui sont sous contrôle des contractants*

*Enquête 2011 AXA , enquête 2007 La Tribune de l'Assurance

Les règlementions qui incitent à mettre en place des stratégies de résilience métier ont émergées dans le sillage du 11 Septembre

Assurance

- Solvency II (Pilier II):
  - Renforcement des exigences sur la gestion des risques et le contrôle interne. Supervision accrue.
  - Prise en compte de tous les risques (souscription, crédit, ***opérationnel***,…)
- Création d'un statut de PSA (Professionnels du Secteur d'Assurance) permettant à des assureurs d'externaliser une partie de leur activité dans un cadre réglementé
- Les conditions générales des contrats d'assurance
  - En vertu de leurs conditions contractuelles avec les clients, les assureurs doivent respecter des délais dans leurs opérations (par ex : délais de prise en charge des sinistres, délais d'indemnisation,…)



- France
  - Code des assurances Article 310-19 et Article 334-8
- Recommandations de l'Autorité de Contrôle Prudentiel

Finance

- Bâle II (bientôt Bâle III), Sarbanes Oxley
- Luxembourg: circulaire CSSF 05/178 sur l'outsourcing

Lois et règlementations européennes

- EU Data Retention laws (Télécommunications), EU Data Protection Act
- EPCIP: programme européen de protection des infrastructures critiques

Normes

- Sécurité ISO 27001, BS 25999 facilitent la mise en place d'un plan de continuité d'activité (PCA)

Sans dispositif de gestion des risques de continuité métier, la Direction Générale peut être tenue pour responsable de toutes pertes qui auraient pu être évitées

Le dispositif de contrôle des risques devra intégrer l'ensemble des réflexions et actions préventives qui permettent de diminuer la fréquence et l'impact d'un sinistre dans l'activité quotidienne de l'entreprise :

- L'ensemble du personnel de l'entreprise est impliqué dans ce dispositif.
- Les mesures de contrôle sont intégrées dans les procédures de traitement.
- La supervision et la cohérence de l'ensemble est assurée par une équipe dédiée pour le compte de la direction générale.
- Des audits périodiques permettent de s'assurer de leur bonne application.

La mise en place d'un **Plan de Continuité d'Activité (PCA)** permet permettra d'apporter une réponse concrète à l'arrêt inattendu d'une partie ou de la totalité des activités de l'entreprise:

- Une organisation de gestion de crise pour traiter les incidents imprévus est définie dans ce dispositif.
- Les modalités de communication de la crise (interne et externe).
- L'ensemble des actions de contournement permettant d'assurer la continuité des activités – notamment les plus critiques.
- Les actions permettant de revenir à la normale.

Le PCA fait partie intégrante de la gestion de crise. Il doit être préparé en amont car les enjeux métiers durant une crise nécessitent des prises de décision en urgence.

Au-delà des obligations légales, réglementaires ou contractuelles, la mise en place d'un PCA permet à la Direction Générale de traiter méthodiquement une situation de crise

1. Garantir la **survie de l'entreprise** en minimisant les impacts financiers, juridiques et d'image d'un sinistre grave
   - Garantir la **sécurité des employées et des actifs**
   - Prioriser les **processus stratégiques** de l'entreprise pour assurer en toutes circonstances **le service minimum** auprès des clients
2. Donner les moyens aux collaborateurs de **pouvoir réagir** en situation de crise
   - Mettre en place des **processus simplifiés** soutenus par une organisation connue de tous
   - Fournir une **documentation claire** et s'assurer de sa **disponibilité**
3. Suivre efficacement la **gestion des sinistres** et en déduire des processus de retour à la normale
   - Définir un **responsable** du Maintien en Condition opérationnelle **reconnu** et **légitime**
   - Eviter que l'activité ne soit **interrompue** plusieurs fois par le même type de **sinistre**

Sommaire

Introduction aux risques de rupture d'activité

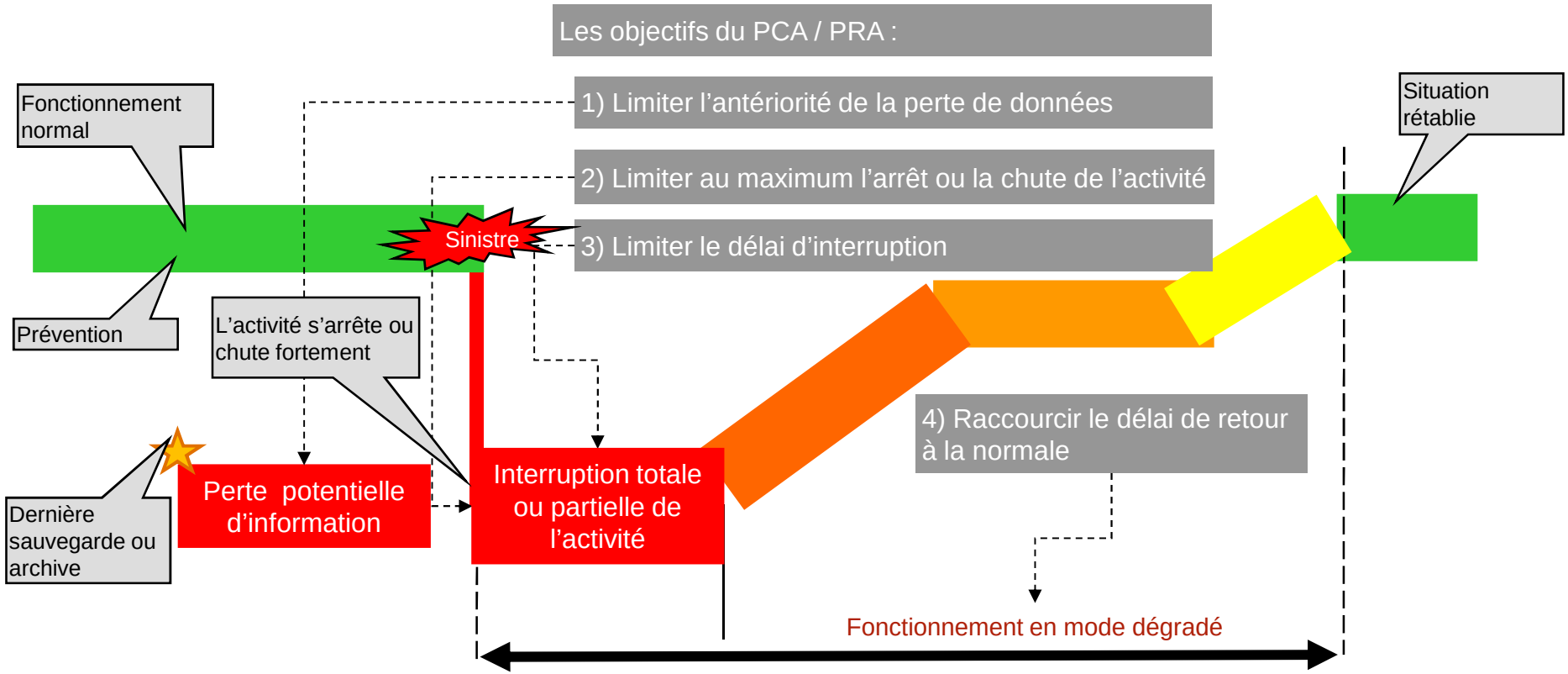
Résilience métier et plan de continuité de l'activité (PCA)

Elaborer et piloter un plan de continuité et de reprise de l'activité

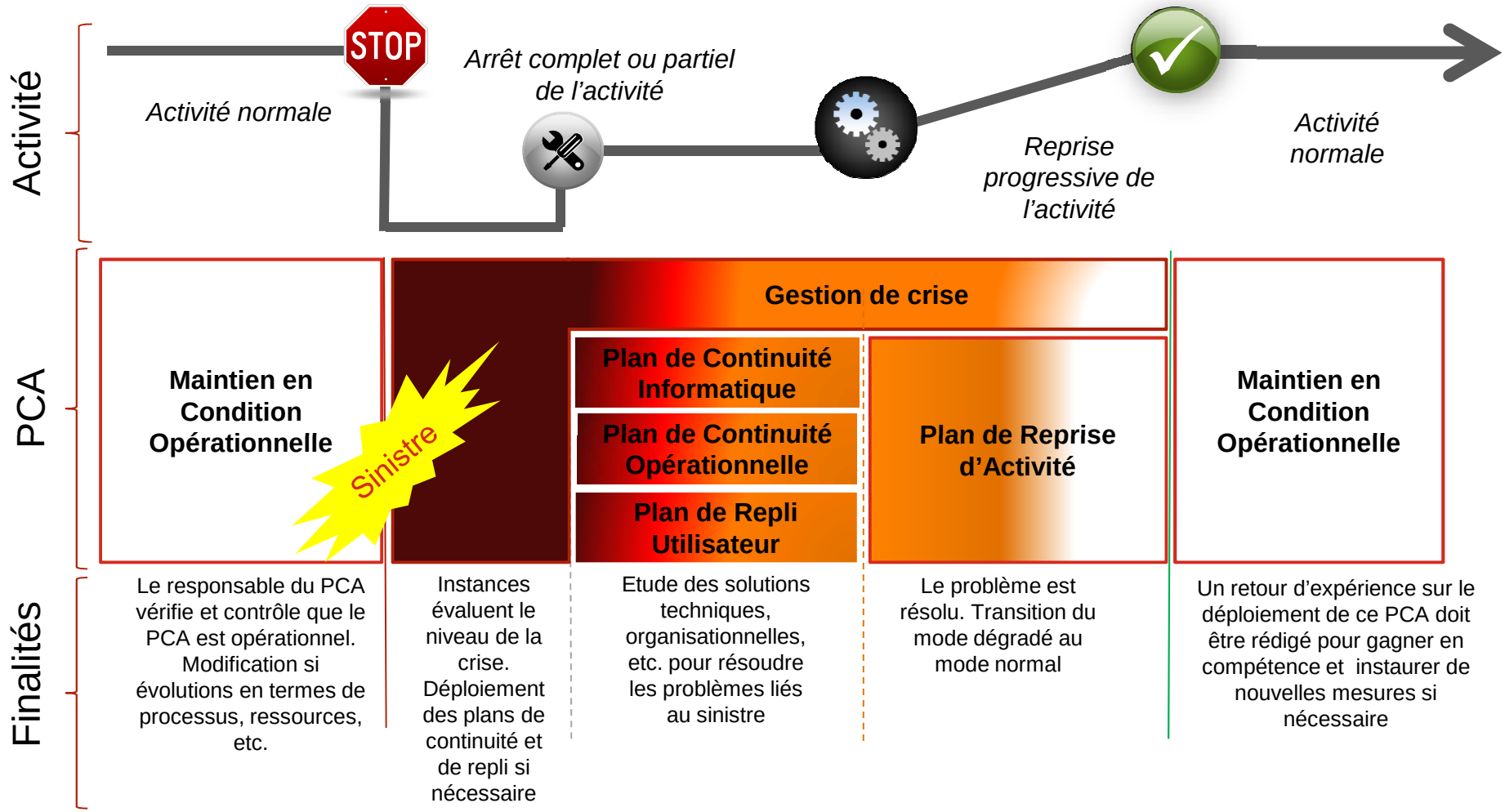
Conclusions

Scénario classique de situation de crise et objectifs du PCA /PRA

- Le PCA / PRA est une approche globale (incluant l'organisation, les procédures et standards, les RH et les systèmes) permettant de s'assurer qu'en cas de sinistre :
  - la perte de données soit réduite à son minimum
  - les opérations clés puissent être poursuivies, même de manière dégradée,
  - et rétablies dans un laps de temps fixé


Les objectifs du PCA / PRA :
1) Limiter l'antériorité de la perte de données
2) Limiter au maximum l'arrêt ou la chute de l'activité
3) Limiter le délai d'interruption
4) Raccourcir le délai de retour à la normale
Fonctionnement normal
Prévention
Sinistre
L'activité s'arrête ou chute fortement
Situation rétablie
Dernière sauvegarde ou archive
Perte potentielle d'information
Interruption totale ou partielle de l'activité
Fonctionnement en mode dégradé

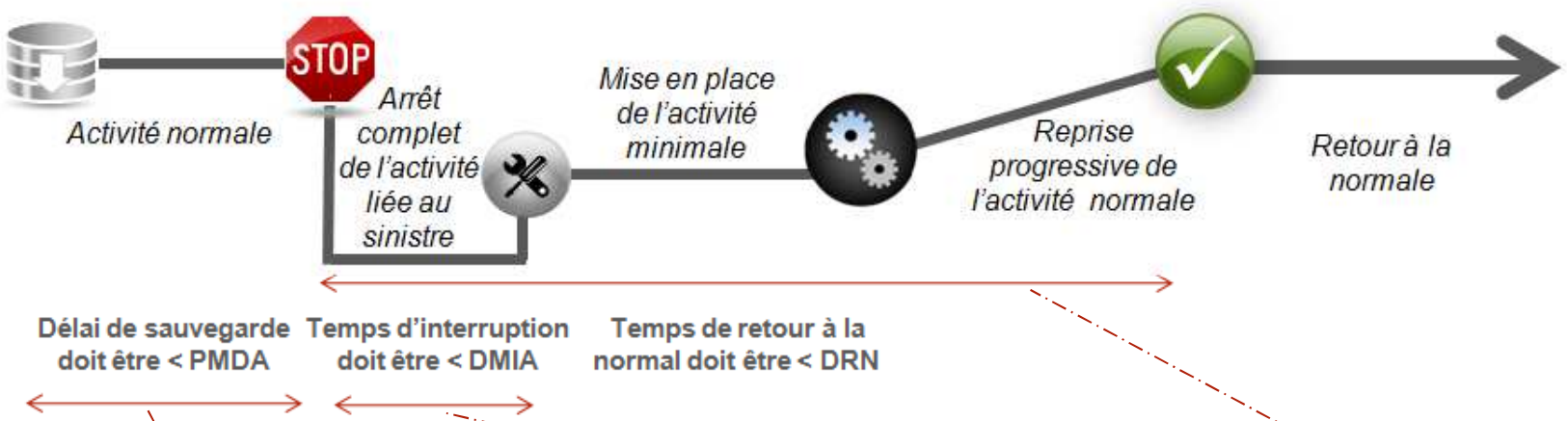
Le PCA/PRA va accompagner les collaborateurs tout au long du sinistre


Activité
PCA
Finalités
STOP
Activité normale
Arrêt complet ou partiel de l'activité
Reprise progressive de l'activité
Activité normale
Maintien en Condition Opérationnelle
Sinistre
Gestion de crise
Plan de Continuité Informatique
Plan de Continuité Opérationnelle
Plan de Repli Utilisateur
Plan de Reprise d'Activité
Maintien en Condition Opérationnelle
Le responsable du PCA vérifie et contrôle que le PCA est opérationnel. Modification si évolutions en termes de processus, ressources, etc.
Instances évaluent le niveau de la crise. Déploiement des plans de continuité et de repli si nécessaire
Etude des solutions techniques, organisationnelles, etc. pour résoudre les problèmes liés au sinistre
Le problème est résolu. Transition du mode dégradé au mode normal
Un retour d'expérience sur le déploiement de ce PCA doit être rédigé pour gagner en compétence et instaurer de nouvelles mesures si nécessaire

En fonction de l'environnement et de l'activité de l'entreprise, les éléments du PCA devront être plus ou moins développés: leur niveau de maturité résulte des choix effectués suite à l'identification des enjeux et des risques lors de l'élaboration du PCA.

L’effort à fournir pour mettre en place un PCA doit être directement proportionnel aux enjeux métiers

Il existe trois indicateurs permettant de **traduire et de prioriser** les besoins métiers. Leur définition permet **d’intégrer un niveau d’exigence** dans les dispositifs de sauvegarde et dans la vitesse d’exécution du PCA


STOP
Activité normale
Arrêt complet de l’activité liée au sinistre
Mise en place de l’activité minimale
Reprise progressive de l’activité normale
Retour à la normale
Délai de sauvegarde doit être < PMDA
Temps d’interruption doit être < DMIA
Temps de retour à la normal doit être < DRN

Perte de données maximale admissible

Durée maximale d'**enregistrement des données** qu'il est acceptable de perdre lors d'une panne (PMDA)

Délai maximal d'interruption admissible

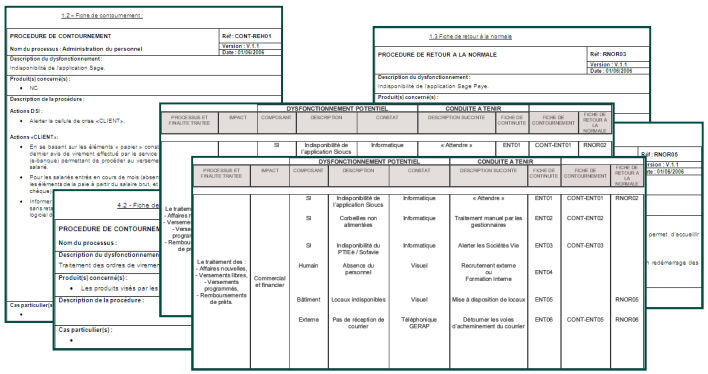
Durée maximale **d'interruption** ; en termes d’outils de production, serveurs, réseaux, applications, ressources (DMIA)

Délai de retour à la normale

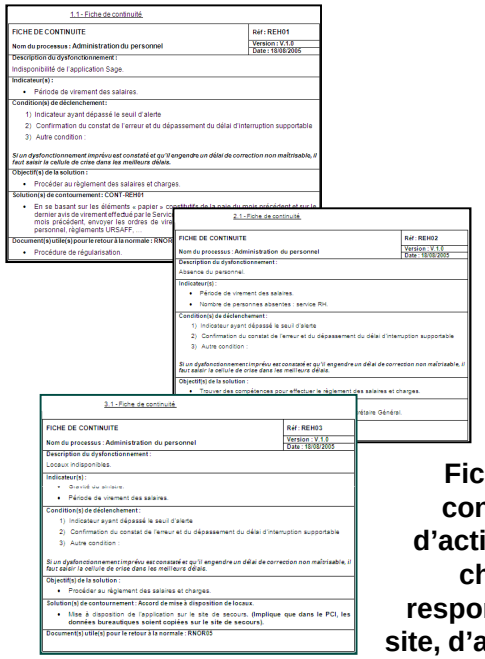
Durée de **baisse d’activité** maximale qui est admissible. (DRN)

Une réflexion sur ces indicateurs permet de définir les processus critiques et leurs priorités mais aussi d’identifier des actions à effectuer en prévention des périodes de crise.

La performance d'un PCA repose sur une base documentaire solide et adaptée aux différents acteurs



Liasse documentaire pour la gestion de crise : liste des risques pris en charge, solutions de contournement, etc.



Fiches de continuité d'activité pour chaque responsable de site, d'activité, etc.

La documentation doit être complète, claire et évolutive lors de la construction du PCA; mais doit se décliner de manière simplifiée pour chaque responsable susceptible de devoir réagir face à un sinistre (responsable d'un site, d'une activité, etc.). Elle devra être disponible avant, pendant et après la période de crise.

Exemple de conception d'un PCA : processus critique « payer les collaborateurs »

1. Calcul des indicateurs : PMDA, DMIA et DRN
2. Priorisé comme étant un processus critique
3.

Ressources	Menaces	Plan d'Actions PCA
Hommes	Des absences Des grèves	Avoir deux sites depuis lesquels il est possible de payer les collaborateurs
Locaux	Incendie Inondation Inaccessibilité (perte des clés)	Posséder un double des clés Avoir un second site
SI	Panne (hard & soft) Virus Electricité	Prévoir du matériel de remplacement sur place
Télécoms	Panne du combiné Perte de tonalité	Prévoir du matériel de remplacement sur place Contractualiser la disponibilité avec les fournisseurs

4. PCA : fiche de continuité d'activité

PROCEDURE DE CONTOURNEMENT — Ref : CONT-REH01 — Version : V 1.1 — Date : 31/08/2006

Nom du processus : Administration du personnel

Description du dysfonctionnement :

Indisponibilité de l'application Sage.

Produit(s) concerné(s) :

Processus : Payer les salaires

Description de la procédure :

Actions DSI :

« En cas d'indisponibilité du SI en fin de mois (panne, bâtiment inaccessible, etc.) payer les salaires sur la base de ceux payés le mois précédent grâce aux classeurs de la salle d'archive (emplacement XXXX) et au chéquier dans le coffre fort (Contacter Mr. XXXXX)»

Actions CLIENTS :

- Informer l'ensemble du personnel de la situation en indiquant que les salaires seront versés sans retard, mais que les outils ne seront rétablis qu'après rétablissement du bon fonctionnement du logiciel de paie

« En cas de panne « physique » du matériel, remplacer les appareils défectueux en suivant le manuel d'installation se trouvant […] s'il s'agit d'un problème de téléphonie, commencer par appeler le N° XXXXXXXX avec le téléphone portable de secours »

Cas particulier(s) :

Sommaire

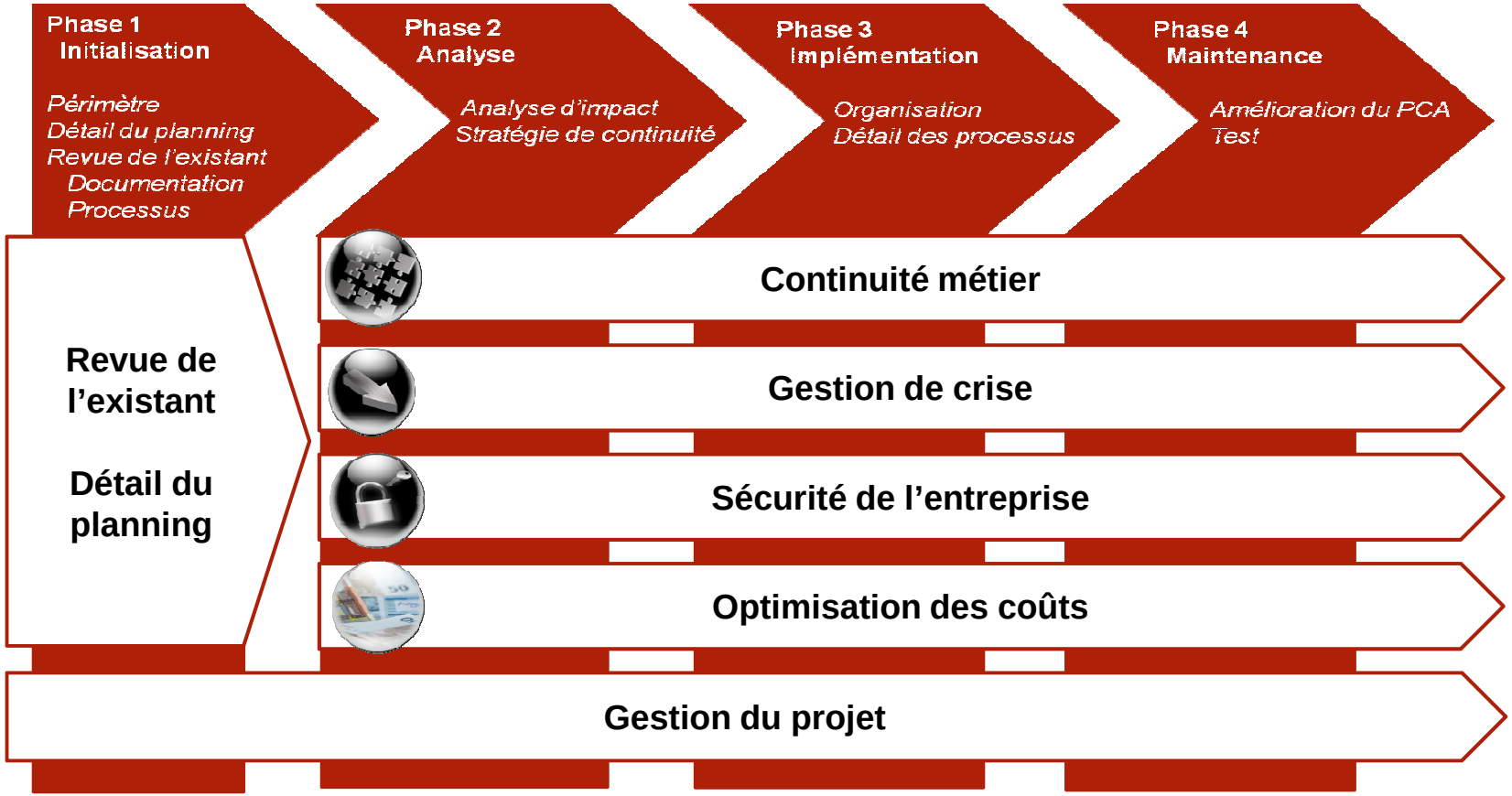
Introduction aux risques de rupture d'activité

Résilience métier et plan de continuité de l'activité (PCA)

Elaborer et piloter un plan de continuité et de reprise de l'activité

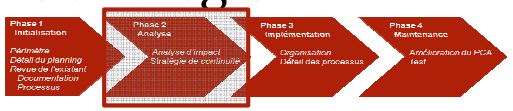
Conclusions

Approche standard pour la création et la mise en place d'une stratégie de gestion de la continuité et reprise des activités.

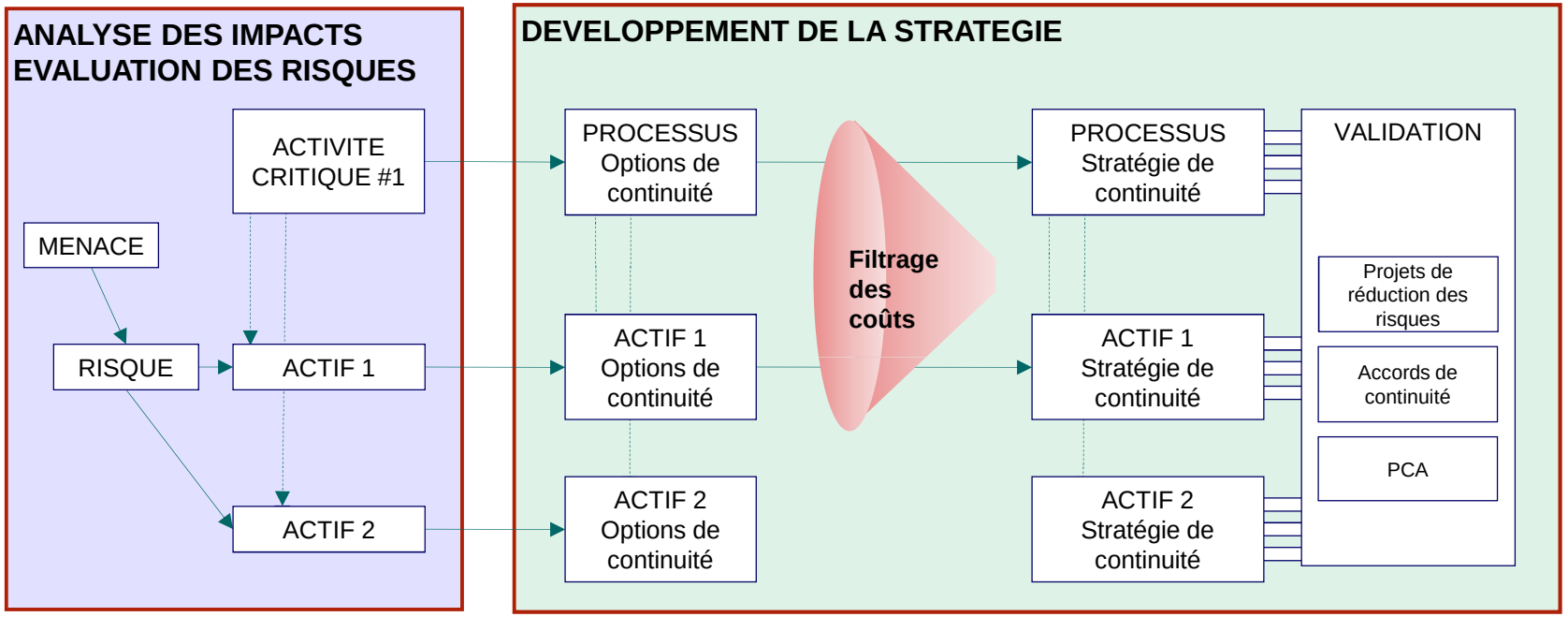


Les meilleures pratiques reposent sur le principe que **tous les risques doivent être listés** mais la mise en place d'un dispositif de maitrise des risques de continuité doit se faire de manière évolutive en **priorisant les processus critiques de l'entreprise.**

Phase 2: **Analyse** des impacts et **développement** d'une stratégie permettant de réduire les risques de continuité



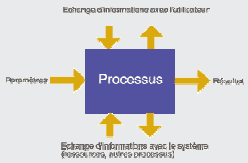
1. Evaluer les conséquences que peut avoir une interruption d'activité (processus ou tâches)
2. Quantifier à partir de quand ces impacts (financiers, légaux..) deviennent intolérables



Service / Fonction	Tâche	Risque global					DMIS	Classement tâche	Risque total
		< 1/2j	< 1j	< 2j	< 5j	< 10j			
Gestion monétaire	Gestion de la trésorerie	3	3	3	3	3	1/2 jour	Critique	36
Gestion monétaire	Contrôle des VL	3	3	3	3	3	1/2 jour	Critique	37
Gestion monétaire	Suivi et contrôle des risques	2	2	2	3	3	1/2 jour	Critique	21
Gestion monétaire	Recherche et analyse	1	1	1	2	3	5 jours	Vitale	11
Gestion monétaire	Passation des ordres	3	3	3	3	3	1/2 jour	Critique	26
Gestion monétaire	Reporting	1	1	1	1	1	> 10 jours	Non sensible	9
Gestion monétaire	Activité commerciale	1	1	2	2	2	2 jours	Vitale	8
Gestion monétaire	Maintenance des SI	3	3	3	3	3	1/2 jour	Critique	20

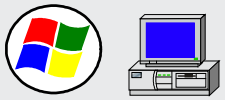
Phase 2: **Développement** d'une stratégie permettant de réduire les risques de continuité identifiés

Processus métier



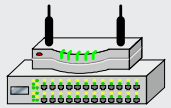
- ✓ Ne rien faire
- ✓ Procédures manuelles
- ✓ Transfert des processus
- ✓ S'assurer sur la perte opérationnelle
- ✓ Arrêt ou modification du service ou produit

Systèmes informatiques



- ✓ Ne rien faire
- ✓ Site de reprise à chaud, à froid, partiel
- ✓ Site de secours mobile
- ✓ Avenants contractuels, sous-traitance

Télécommunications



- ✓ Ne rien faire
- ✓ Connections réseaux redondantes
- ✓ Routage alternatif via un fournisseur externe
- ✓ Fournisseur externe

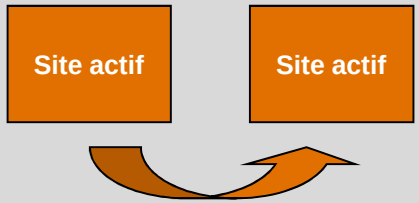
Données vitales

- ✓ Ne rien faire
- ✓ Stockage miroir
- ✓ Sauvegarde journalière
- ✓ Archivage et stockage en externe + SLA

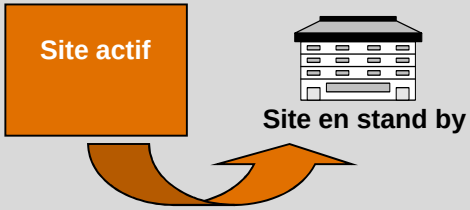
Activités externalisées

- ✓ Ne rien faire
- ✓ Stratégie d'externalisation alternative
- ✓ Stratégie de fournitures de produits et de services alternative

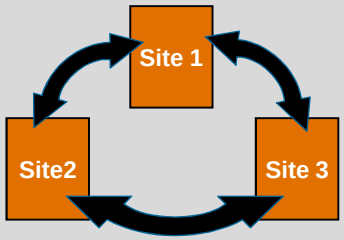
Modèle haute disponibilité



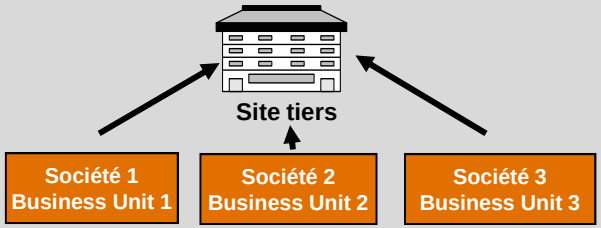
Modèle traditionnel



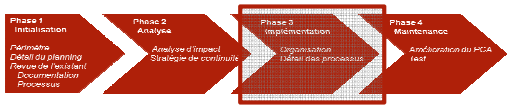
Modèle opérationnel partagé



Modèle externalisé



Phase 3: Implémentation de la stratégie de réduction des risques de continuité identifiés



IMPLEMENTER LES PROJETS DE REDUCTION DES RISQUES ET ACCORDS DE REPRISE

1. Mettre en place les projets de réduction des risques

2. Mettre en place les accords relatifs aux plans de reprise

OBJECTIF:
S'assurer que les mesure de réduction du risques sont mises en place

DEVELOPPEMENT DE PROCEDURES DE REPONSE (PLAN DE GESTION DE CRISE)

3. Mettre en place l'ensemble de la structure pour le PCA

4. Définir les procédures d'identification, de notification et de déclenchement

OBJECTIF:
Fournir la possibilité de répondre à un incident et lancer le PCA

DEVELOPPEMENT DES PLANS DE REPRISE

5. Développer les plans de reprise pour les processus et les actifs associés

6. Développer les procédures temporaires dans le cadre d'une reprise

7. Développer les procédures de retour à la normale

OBJECTIF:
Définir les procédures détaillées

TESTER ET VALIDER LES PLANS

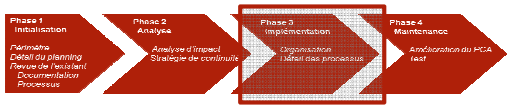
8. Réaliser des tests de validation

9. Documenter les résultats des tests et identifier les mise à jour nécessaire sur les plans

10. Obtenir l'approbation de la direction

OBJECTIF: S'assurer que les plans sont fiables et opérationnels

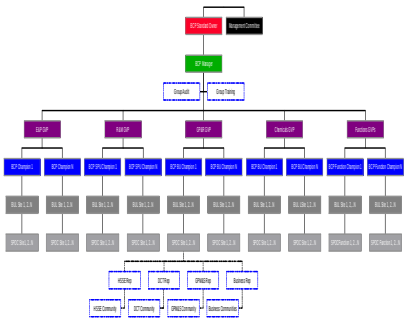
Phase 3: Exemple de la dynamique d'une gestion de crise



Crise

Déclencher l'alerte
Activer les plans requis afin de gérer l'incident

Notifier
Personnes à avertir lors d'une crise



Création d'une organisation de crise

Activation cellule de crise

Evaluation de la crise
Mise à jour de l'état du personnel, des moyens techniques, de l'infrastructure

Activer le plan de secours

Exécuter Plan de Continuité d'Activité

Démarrer la reprise
Réaliser les étapes de reprise et suivre son avancement

Phase 4: assurer le maintien opérationnel du PCA

FORMATION ET SENSIBILISATION

1. Assurer en permanence formation et sensibilisation du personnel

OBJECTIFS: S'assurer que le personel et les partenaires externes sont conscient et comprennent leur roles dans l'execution du PCA

PROCEDURES DE MAINTENANCE

2. Définition des principes organisationnels de maintien opérationnel du PCA

3. Création des procédures de mise à jour du plan et outils de reporting

4. Définition de la stratégie de test

5. Maintenance effective du PCA et de ses composantes fondamentales (Plan de secours Informatique, gestion de crise, reprise des moyens techniques et des activités Métier)

6. Définir un programme de test régulier, de maintenance, d'audit des plans de continuité d'activité

7. Mise en place d'un processus d'amélioration continue de « gestion de crise » - Industrialisation et pérennisation des processus

OBJECTIFS: S'assurer que le PCA est maintenu et mis à jour et continue d' être en ligne avec les besoins métiers

VALIDATION DU PCA

8. Approbation de la direction

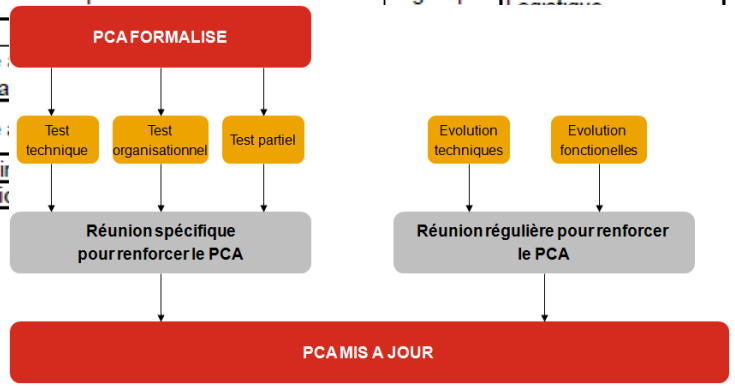
OBJECTIFS: Valider la mise à jour du PCA

Le plan doit être revu et mis à jour régulièrement (au moins une fois par an) pour tenir compte de l'évolution des activités, de la technologie et de la stratégie de l'entreprise.

Phase 4: maintenance et test du PCA

Le plan de continuité doit être testé régulièrement (revue des procédures, jeu de rôles, test grandeur nature réel ou « à blanc »…), et ce à chaque introduction d'une application / infrastructure informatique nouvelle ou réorganisation.

PHASE	Actions	Acteurs	Document associé	Résultats attendus	Testeur	document support de test
Survenance du sinistre et prise de décision de la cellule de crise	Se rendre sur le point de ralliement	Métiers	Procédure métier	Le point de raliement est connu	Métiers	Protocole de test Métiers
	Passage des consignes	Métiers	Procédure métier	1. Les moyens de communication fonctionnent 2. Les coordonnées sont à jour	Métiers	Protocole de test Métiers
Activation du secours	***Sur site de secours***					
	Déploiement des socles sur les postes	DSI	Procédure DSI	Poste de travail configuré	DSI	Protocole de test DSI
	Connexion aux imprimantes	DSI	Procédure DSI	Imprimantes configurées et fonctionnelles	DSI	Protocole de test DSI
	Installation des applications atypiques	DSI	Procédure DSI	Applications atypiques installées	DSI	Protocole de test DSI
	Connexion au site informatique central	DSI	Procédure DSI	Connexion aux applications centrales	DSI	Protocole de test DSI
	Connexion aux données bureautiques et applications locales (restauration de serveur…)	DSI	Procédure DSI	Accès aux données bureautiques et aux applications locales	DSI	Protocole de test DSI
	Bascule des numéros de téléphone	Téléphonie	Procédure Téléphonie	Appel transmis sur le site de secours	Téléphonie	Protocole de test Téléphonie
	Bascule des numéros de fax	Téléphonie	Procédure Téléphonie	Fax transmis sur le site de secours	Téléphonie	Protocole de test Téléphonie
	Mise à disposition du matériel requis	Logistique	Procédure Logistique	Matériel disponible	Logistique	Protocole de test DSI
	Mise à disposition des fournitures requises	Logistique	Procédure Logistique	Fourniture disponible	Logistique	Protocole de test
	Sur site Interne					
	Déplacement des collaborateurs si nécessaires	Logistique	Procédure Logistique	Mise … arriva…		
	Installation des postes de travail ou paramétrage des postes existants	DSI	Procédure DSI	Mise …		
	Connexion aux imprimantes	DSI	Procédure DSI	Impri…		
	Installation des applications atypiques	DSI	Procédure DSI	Appli…		



Sommaire

Introduction aux risques de rupture d'activité

Résilience métier et plan de continuité de l'activité (PCA)

Elaborer et piloter un plan de continuité et de reprise de l'activité

Conclusions

Les facteurs clé de succès de la mise en place d'un PCA

Les bonnes pratiques autours de la mise en place d'un PCA portent sur quatre axes: la gouvernance, la prise en compte des besoins métiers, l'adéquation coûts engagés vs. risques encourus et une stratégie de maintient en continuité opérationnelle efficace.

1 **Une Gouvernance Claire**

- Obtenir **l'implication du comité** de direction
- Une **mobilisation** des collaborateurs internes

2 **L'implication forte des métiers**

- Avoir des relais de **haut niveau de séniorité** dans les départements métiers
- Définir les **processus critiques**
- Accéder **aux documentations** des processus

3 **Analyser les coûts vs. risques**

- Juger de la **réalité des risques,** vérifier l'adéquation entre les investissements prévus et **les risques encourus**
- Procéder à un arbitrage fonds propres / assurance
- Intégrer les risques liés aux clients et aux partenaires

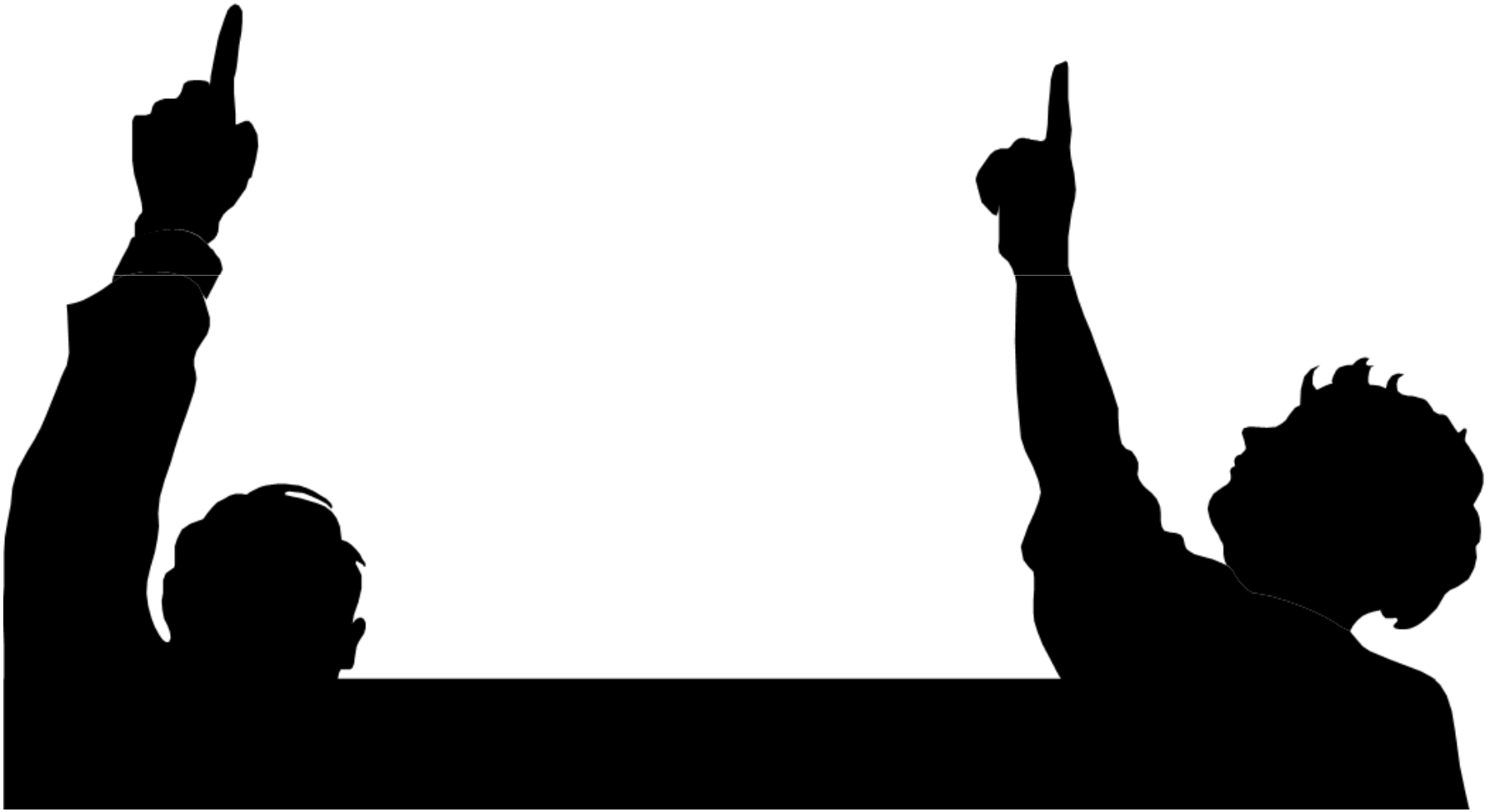
4 **Pérennité de la continuité opérationnelle**

- **Identifier un responsable** pour le pilotage efficace et le maintien des outils
- **Faire vivre** le PCA : le tester régulièrement et le diffuser aux acteurs concernés
- **Sensibiliser** tous les collaborateurs et les **former si nécessaire**
- Intégrer les **retours d'expérience marché** et **penser amélioration continue**

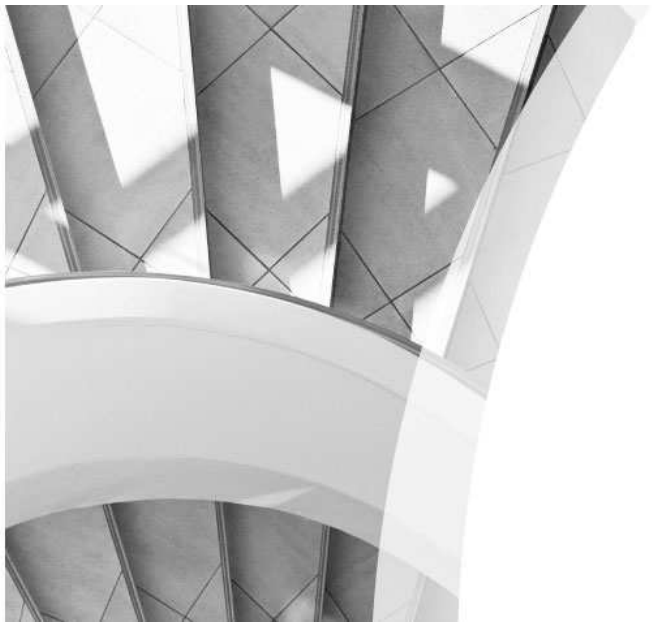
Les challenges à venir

- **Pour le secteur de l'assurance**
  - Solvency II, imposant de nouvelles pratiques en matière de gestion du risque opérationnel. Identifier le bon niveau d'équilibre entre exigence de fonds propres et assurance dans le cadre de la gestion de la continuité métier
  - Pour les clients et leur polices d'assurance « perte d'exploitation ». Etablir des contrats d'assurance et des conditions tarifaires (primes et franchises) sur base de la présence d'un PCA client. Comment évaluer l'efficacité réelle des ces PCA? En se dotant de capacités d'audit / conseil spécialisées?
- **En général – remise en cause des PCA existants du fait de…**
  - L'émergence du « ***cloud-computing*** »
    - Stockage de données auprès de tiers (Data as a Service)
    - Utilisation de plateformes logicielles auprès de tiers (Software as a Service)
  - Les nouveaux besoins liés à la ***mobilité en entreprise***
    - Utilisation de nouveaux outils de travail ou de communication
    - Itinérance des employés générant de nouveaux risques (sécurité notamment)
  - Le développement de ***nouveaux modèles opératoires***, notamment mondiaux et globalisés
    - Centres de service partagés informatique ou métier desservants des groupes au niveau mondial
    - Externalisation de processus métiers (BPO), parfois auprès de multiples prestataires
    - Exposition à des risques connus mais probabilité d'occurrence / impacts mal maîtrisés ou sous-estimés

Questions / Réponses



Contacts Kurt Salmon
Centre d'expertise PCA / PRA



Kurt Salmon Luxembourg, 41, Zone d'Activité Am Bann,

L-3372 Leudelange, Luxembourg

T +352 26 37 74 1 **F** +352 26 37 74 982

www.kurtsalmon.com

Loic DUNAND
Associate Partner
CIO Advisory

Kurt Salmon

41, Zone d'Activité Am Bann,
L-3372 Leudelange,
Luxembourg

Mobile: +352 661 320 357
loic.dunand@kurtsalmon.com

Patrice PASSE-COUTRIN
Manager
CIO Advisory

Kurt Salmon

41, Zone d'Activité Am Bann,
L-3372 Leudelange,
Luxembourg

Mobile: +352 661 321 457
patrice.passe-coutrin@kurtsalmon.com